

# Protecting Production:

## A Window Into Legacy Systems

Securing the legacy challenge at the heart of Europe's pharma OT environments

From molecule to market, legacy Windows systems remain deeply embedded in validated processes across Europe's shopfloors. But with ongoing support expiring and advanced threats evolving, these systems pose an increasing risk to uptime, compliance and future OT security. The question is: what does the OT legacy landscape look like for today's pharma manufacturers—and just how exposed are they?

Based on exclusive TXOne research from over 530 OT and ICS cybersecurity decision-makers across eight European industrial sectors, the following insights reveal the scale of pharma's reliance on legacy Windows OS and how organisations are considering a future where legacy lives on, protected.

### A Targeted Threat

With complex OT systems and a reliance on legacy systems exposing weak points to exploit high-value Intellectual property (IP), Europe's pharma industry ranks as the...

**2nd**  
Most impacted victim of "the top three ransomware actors"

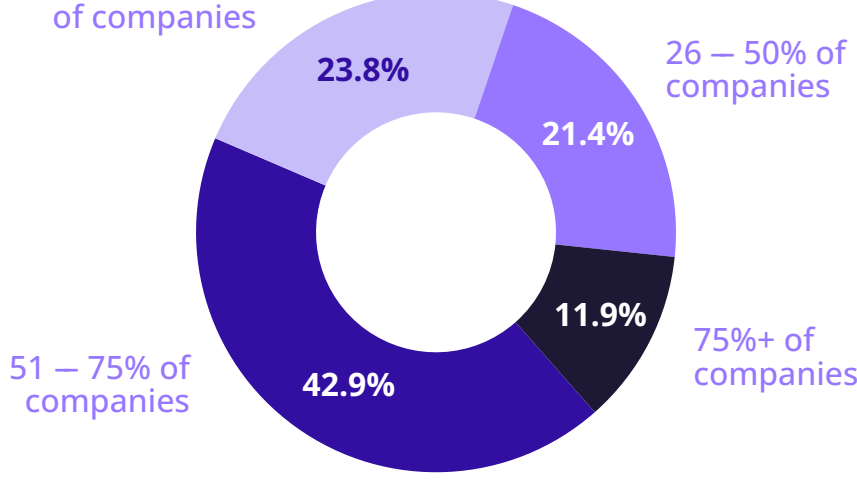
**2nd**  
Highest sector to experience a "breach or theft of data"

**3rd**  
Most targeted entity by threat actors

The real kicker? It also ranks as the third most impacted sector to witness a "disruption of services not related to healthcare", with primary disruptions identified as...



Yet over half of pharma manufacturers still rely on legacy Windows systems to deliver at least 51%+ of their OT environments.



### The number one reason

**59%**

Compatibility with legacy equipment

### Risk versus Reality

For OT and cybersecurity leaders, the top 3 business challenges associated with legacy Windows systems in OT environments were:



While their Top 3 cybersecurity concerns honed in on Malware/virus infections, unauthorised access, and a lack of patching or updates. And yet...

**28.6%** ...had experienced a cybersecurity incident involving legacy Windows systems in the past 12 months.

### So why the mismatch?

The risk isn't overstated. Instead, the threat landscape is evolving faster than legacy systems can detect or support.

### With an increasing latent risk profile, many legacy OT systems:

- Lack real-time monitoring**, meaning breaches may go unreported
- Are air-gapped or segmented**, giving a false impression of immunity
- Prioritise uptime and validation over security**, delaying detection or disclosure

'System performance impact' was the top concern for OT and cybersecurity leaders when implementing security measures into OT environments, with...

**64.3%** having implemented network segmentation

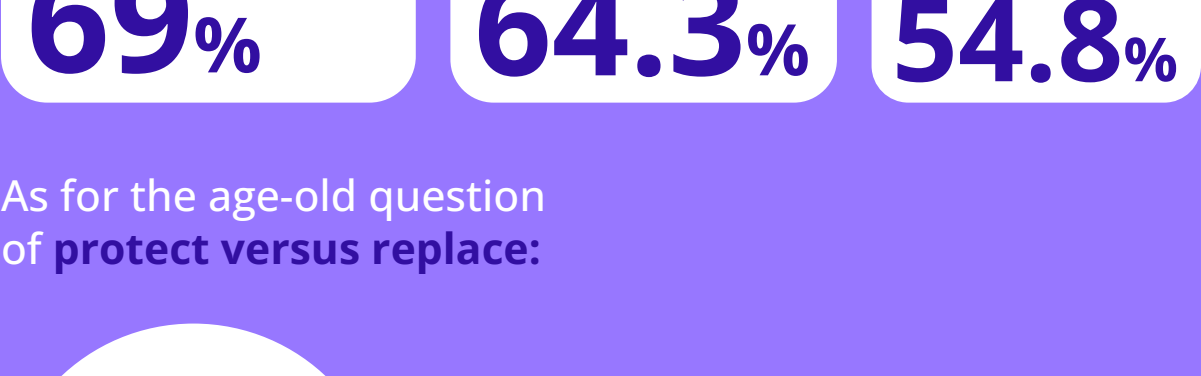
**59.5%** added endpoint protection tools

**45.2%** included continuous monitoring

...to protect legacy Windows systems.

### Protecting Legacy

Two-thirds of pharma manufacturers were likely to invest in a cybersecurity solution designed specifically to protect legacy Windows systems, and were most influenced by:



As for the age-old question of protect versus replace:

**64.3%** Consider upgrading legacy systems at least 25% more expensive than implementing a cybersecurity solution to protect them.

### For most, replacing legacy Windows OS means:

- Risk of production downtime
- Long rollout timelines
- Costly recertification & validation
- High upfront hardware & software costs

### A Diagnosis Without Disruption

Trusted to secure the operations of more than 5,000 organisations globally with cybersecurity solutions tailored for ICS and OT environments, TXOne's OT-native solutions protect legacy endpoints without disrupting validated processes.

Seamlessly integrating with existing OT infrastructure and all Windows systems, our Zero Trust approach ensures that legacy doesn't have to mean vulnerability for Europe's pharmaceutical industry.

For a deeper dive into securing Europe's pharma OT environments, get your copy of our eBook, 'Prescribing Cyber Resilience'.

[Download](#)

**Start Protecting What Matters. Your Legacy.**

Discover how TXOne can secure your organisation with OT-native solutions tailored to your existing infrastructure. Get in touch, today.

[Let's talk](#)